What is claimed is:

[Claim 1] 1. A computer program for assisting a user to determine whether a hyperlink to a target uniform resource locator (URL) is spoofed, the method comprising:

a code segment that listens with a computerized system for an activation of the hyperlink;
a code segment that extracts an originator identifier and encrypted data from the hyperlink;
a code segment that decrypts said encrypted data into decrypted data based on said originator identifier;
a code segment that presents information on a display unit;
a code segment that redirects; and
a code segment that determines whether the hyperlink includes said originator identifier and said encrypted data decrypts successfully, and then:

runs said code segment that presents, to present a confirmation of authentication to the user conveying the name of the owner and the domain name of the target URL, and

runs said code segment that redirects, to redirect the user to the target URL;

and otherwise, runs said code segment that presents, to present a warning dialog to the user.

[Claim 2] 2. The computer program of claim 1, wherein the computer program is digitally signed.

[Claim 3] 3. The computer program of claim 1, wherein said code segment that listens runs as a service in said computerized system.

[Claim 4] 4. The computer program of claim 1, wherein said code segment that listens includes a hypertext transport protocol (HTTP) server.

[Claim 5] 5. The computer program of claim 1, wherein said code segment that listens listens at a preset non routable internet protocol (IP) address and at a preset port.

[Claim 6] 6. The computer program of claim 1, wherein said code segment that decrypts includes a code segment that extracts the target URL from said decrypted data.

[Claim 7] 7. The computer program of claim 1, wherein said the hyperlink includes the target URL and said code segment that decrypts includes:

a code segment that extracts a digital signature from said decrypted data; and
a code segment that verifies said digital signature against said originator identifier.

[Claim 8] 8. The computer program of claim 1, wherein said code segment that decrypts employs a public key associated with said originator identifier.

[Claim 9] 9. The computer program of claim 1, further comprising:

a code segment that matches said originator identifier to one of a plurality of registered originators; and
a code segment that retrieves a decryption key associated with said originator identifier for use by said code segment that decrypts.

[Claim 10] 10. The computer program of claim 1, wherein said code segment that presents employs a dialog box that only software running locally in said computerized system can provide, thereby avoiding confusion with a remotely generated browser window.

[Claim 11] 11. A system for assisting a user to determine whether a hyperlink to a target uniform resource locator (URL) is spoofed, the system comprising:

a computerized system having a display unit;
a logic in said computerized system that listens for activation of the hyperlink;
a logic that extracts an originator identifier and encrypted data from the hyperlink;
a logic that decrypts said encrypted data into decrypted data based on said originator identifier;
a logic that determines whether the hyperlink includes said originator identifier and that said encrypted data decrypts successfully;

a logic responsive to said logic that determines, that presents on said display unit a confirmation of authentication conveying the name of the owner and the domain name of the target URL and that redirects the user to the target URL; and
a logic responsive to said logic that determines, that presents on said display unit a warning dialog to the user.

[Claim 12] 12. The system of claim 11, wherein said logic that listens runs as a service.

[Claim 13] 13. The system of claim 11, wherein logic that listens includes a hypertext transport protocol (HTTP) server.

[Claim 14] 14. The system of claim 11, wherein said logic that listens listens at a preset non routable internet protocol (IP) address and at a preset port.

[Claim 15] 15. The system of claim 11, wherein said logic that decrypts includes a logic that extracts the target URL from said decrypted data.

[Claim 16] 16. The system of claim 11, wherein said the hyperlink includes the target URL and said logic that decrypts includes:

a logic that extracts a digital signature from said decrypted data; and
a logic segment that verifies said digital signature against said originator identifier.

[Claim 17] 17. The system of claim 11, wherein said logic that decrypts employs a public key associated with said originator identifier.

[Claim 18] 18. The system of claim 11, further comprising:

a logic that matches said originator identifier to one of a plurality of registered originators; and
a logic that retrieves a decryption key associated with said originator identifier for use by said logic that decrypts.

[Claim 19] 19. The system of claim 11, wherein said logic that presents employs a dialog box that only software running locally in said

computerized system can provide, thereby avoiding confusion with a remotely generated browser window.

[Claim 20] 20. A method for assisting a user to determine whether a hyperlink to a target uniform resource locator (URL) is spoofed, the method comprising:

listening for an activation of the hyperlink;
extracting an originator identifier and encrypted data from the hyperlink;
decrypting said encrypted data into decrypted data based on said originator identifier;
when the hyperlink includes said originator identifier and said encrypted data decrypts successfully:
presenting a confirmation of authentication to the user, wherein said confirmation of authentication conveys the name of the owner and the domain name of the target URL; and
redirecting the user to the target URL;
and otherwise, presenting a warning dialog to the user.

[Claim 21] 21. The method of claim 20, wherein said listening includes running at least one of a service and a hypertext transport protocol (HTTP) server in a computerized system.

[Claim 22] 22. The method of claim 20, wherein said listening is at a preset non routable internet protocol (IP) address and a preset port.

[Claim 23] 23. The method of claim 20, said decrypting includes extracting the target URL from said decrypted data.

[Claim 24] 24. The method of claim 20, wherein said the hyperlink includes the target URL and said decrypting includes:

extracting a digital signature from said decrypted data; and
verifying said digital signature against said originator identifier.

[Claim 25] 25. The method of claim 20, further comprising:

matching said originator identifier to one of a plurality of registered originators;
retrieving a decryption key associated with said originator identifier for use in said decrypting.

[Claim 26] 26. The method of claim 20, wherein said presenting a confirmation employs a dialog box that only software running locally in a computerized system can provide, thereby avoiding confusion with a remotely generated browser window.